Doxxing, swatting and the new trends in online harassment

April 22 2015, by Andrew Quodling

When the SWAT team bursts into your bedroom, it’s not only unpleasant but potentially deadly. Credit: Jason Eppink/Flickr, CC BY

Imagine this: there's a knock at your door. "Pizza delivery!" It's the fifth time in the last hour that you've had to say to a delivery-person: "No, I really didn't order anything." That's irritating.

Half an hour later, there's another noise at the door. This time it's forced open as your house is stormed by the heavily armed and aggressive special response unit of your local police force. They're responding to a

tip off that warned them of a hostage situation at your address. That's not just irritating. That's dangerous.

Why is all this happening? Turns out, you've come to the attention of a cluster of mischief makers and misanthropes in one of the internet's dank corners.

You've been "doxxed". Your private information has been posted, perhaps by an anonymous imageboard user, who's implored others to "do with it as you will".

This might sound far-fetched, but these sorts of internet-enabled attacks have become more frequent in recent years. In fact, the Federal Bureau of Investigation has been cautioning citizens about "swatting" (see below) since 2008.

It has become common to see articles about how these attacks have affected politicians (both Republican and Democrat in the US), celebrities, journalists, businesses, video game streamers and public servants.

What is doxxing?

Doxxing – named for "documents" or "docs" – is the act of release of someone's personal and/or identifiable information without their consent. This can include things like their full legal name, social security numbers, home or work addresses and contact information.

There's no set format for a "dox"; the doxxer simply publishes whatever information they've managed to turn up in their searches. Sometimes this even includes the names and details of their target's family or close friends.

As a tactic of harassment, doxxing serves two purposes: it intimidates the people targeted by invading and disrupting their expectations of privacy; and it provides an avenue for the perpetuation of that person's harassment by distributing information as a resource for future harassers to use.

Technology and security expert Bruce Schneier argues that 2015 will see even more doxxings, as "everyone from political activists to hackers to government leaders has now learned how effective this attack is".

What is swatting?

Swatting – named for the US police Special Weapons And Tactics (SWAT) teams – is the act of making a false report to the police with the intention of having a heavily armed response team sent to the target's home.

This is made even more problematic by the militarisation that local US police forces have undergone in the last decade through initiatives like the Department of Defense's *1033 program*, which allows the pentagon to provide military grade weapons and equipment to local police forces on a free, permanent loan.

Technology journalist Sarah Jeong describes this as "assault by proxy", as the police can cause serious injury to the targets of these swatting attacks.

How do these attacks happen?

Unfortunately, the technical barrier to doxxing or swatting a person is low. A doxxer can acquire information on their target through a variety of legitimate public sources. Or, more nefariously, through social

engineering techniques.

Swatting often just requires the name, phone number and address of the intended target. Swatters often use cheap or freely available anonymising technology to disguise their identity, or to "spoof" the phone number of their target, when making their false report—a move that makes their crime difficult to police.

These attempts also prey on the good faith basis with which emergency responders treat their callers, and as a result valuable police time and resources are diverted away when they may be needed elsewhere.

How can you protect yourself?

If you find yourself at the receiving and of these forms of intimidation and abuse, you've likely done nothing wrong. People are doxxed and swatted for all sorts of imagined wrongs, as banal as having an opinion on the internet or playing video games.

Unfortunately, the prevalence of doxxing and swatting is, in part, born of a perfect storm in personal data insecurity and easily-abused systems for reporting crime. There are no perfect solutions for avoiding being doxxed or swatted except making yourself a more difficult target by adopting strong information security practices.

While the simplest solution for online security is not having online data, this is impractical in the digital age because major parts of our social and professional lives are intermediated through web services. That said, there are a few precautions you can take to increase the security of your data online.

Google yourself

One of the first steps in securing your personal details is discovering to what extent they're already out-there and publicly available. If you find old accounts or websites you no longer want, sites like justdelete.me can provide information about having your account deleted from certain websites.

Don't re-use passwords for multiple services

This can be difficult, as a new password for every service you use will be taxing to even the best of memories. The best, most complex passwords will be challenging to guess or to brute-force, but also difficult to remember.

Here's where technology can make life easier; a password manager app, like LastPass, KeePass or 1Password can help you set unique, complex passwords for each service you use, and let you secure them behind a single, more memorable password.

Though password managers come with their own risks, I'd argue that the benefits of using complex passwords can outweigh these.

Turn on two-factor authentication

Two-factor authentication requires that people trying to access your account have access to a password as well as a "trusted device" – typically your mobile phone – in order to receive an authentication code before gaining access to your account. The Two Factor Auth website lists popular web services and their support (or lack of support) for two factor authentication.

You can find more information in advice from people who've experienced these attacks, and at websites like Crash Override Network,

a support network for the targets of online abuse that provides some excellent guides on online security, and how to cope with doxxing and swatting attacks.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation